

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----		X	
HENRY PLATSKY,		:	
		:	
	Plaintiff,	:	
-v-		:	20 Civ. 573 (JPC) (SN)
		:	
FEDERAL BUREAU OF INVESTIGATION,		:	
		:	
	Defendants.	:	
-----		X	

DECLARATION OF MICHAEL G. SEIDEL

I, Michael G. Seidel, declare as follows:

(1) I am the Section Chief of the Record/Information Dissemination Section (“RIDS”), Information Management Division (“IMD”), Federal Bureau of Investigation (“FBI”), Winchester, Virginia. I joined the FBI in September 2011, and prior to my current position, I was the Assistant Section Chief of RIDS from June 2016 to July 2020; Unit Chief, RIDS Litigation Support Unit from November 2012 to June 2016; and an Assistant General Counsel, FBI Office of General Counsel, Freedom of Information Act (“FOIA”) Litigation Unit, from September 2011 to November 2012. In those capacities, I had management oversight or agency counsel responsibility for FBI FOIA and Privacy Act (“FOIPA”) litigation cases nationwide. Prior to my joining the FBI, I served as a Senior Attorney, U.S. Drug Enforcement Administration (“DEA”) from September 2006 to September 2011, where among myriad legal responsibilities, I advised on FOIPA matters and served as agency counsel representing the DEA in FOIPA suits nationwide. I also served as a U.S. Army Judge Advocate General’s Corps Officer in various assignments from 1994 to September 2006 culminating in my assignment as Chief, General Litigation Branch, U.S. Army Litigation Division where I oversaw FOIPA

litigation for the U.S. Army. I am an attorney registered in the State of Ohio and the District of Columbia.

(2) In my official capacity as Section Chief of RIDS, I supervise approximately 238 FBI employees, supported by approximately 94 contractors, who staff a total of twelve (12) Federal Bureau of Investigation Headquarters (“FBIHQ”) units and two (2) field operational service center units whose collective mission is to effectively plan, develop, direct, and manage responses to requests for access to FBI records and information pursuant to the FOIA as amended by the OPEN Government Act of 2007, the OPEN FOIA Act of 2009, and the FOIA Improvement Act of 2016; the Privacy Act of 1974; Executive Order 13526; Presidential, Attorney General, and FBI policies and procedures; judicial decisions; and Presidential and Congressional directives. The statements contained in this declaration are based on my personal knowledge, upon information provided to me in my official capacity, and upon conclusions and determinations reached and made in accordance therewith.

(3) Because of the nature of my official duties, I am familiar with the procedures followed by the FBI in responding to requests for information from its files pursuant to the provisions of the FOIA, 5 U.S.C. § 552 and the Privacy Act, 5 U.S.C. § 552a. Specifically, I am aware of the FBI’s handling of Plaintiff’s Freedom of Information/Privacy Acts (“FOIPA”) requests to the FBI for records pertaining to himself.

(4) The FBI submits this declaration in support of Defendant’s motion for summary judgment, and provides the Court with a summary of the administrative history of Plaintiff’s requests; the procedures used to search for responsive records; and the FBI’s justification for withholding information in part or in full pursuant to Privacy Exemption (j)(2), 5 U.S.C. § 552a (j)(2) and FOIA Exemption 7(E), 5 U.S.C. § 552 (b)(7)(E).

ADMINISTRATIVE HISTORY OF PLAINTIFF'S REQUESTS

FBI FOIPA REQUEST NUMBER 1412680-000

(5) By letter dated July 17, 2018, Plaintiff submitted a FOIPA request to the FBI seeking information concerning his name on “any watch lists brought by the FBI” relating to an alleged meeting between representatives of the FBI and “three New York emergency service departments” that took place “in the run-up to the 1st Gulf War.”¹ (Ex. A.)

(6) By letter dated August 6, 2018, the FBI informed Plaintiff it had assigned his request FOIPA Request Number 1412680-000. Additionally, the FBI informed him it had completed its search for records responsive to his request, which the FBI interpreted broadly to seek documents on which Plaintiff's name appeared. The FBI further informed him that records potentially responsive to his request (i.e., records on which Plaintiff's name appeared) had previously been sent to the National Archives and Records Administration (“NARA”).² The FBI advised if Plaintiff wished to review these records, he could send his request to NARA using file number[s] 100-HQ-446284 and 100-NY-157576 as a reference.³ Also, the FBI informed Plaintiff, since these records were not reviewed, it is not known if they are actually responsive to

¹ Although Plaintiff provides information concerning a “meeting that the FBI set with what were then three New York City emergency service departments in the run-up to the first Gulf War in 1990,” “the purpose of [which] was to set up a Joint Anti-Terrorism Task Force between the FBI and the three departments,” it is not entirely clear what relationship exists between that meeting and his name on “any watch lists brought by the FBI.” However, Plaintiff does provide under penalty of perjury his legal name, date of birth, place of birth, email address, and current address as personal identifiers to his request, and the FBI interpreted his first FOIA request broadly to seek documents on which Plaintiff's name appeared.

² Record retention and disposal is carried out under supervision of the NARA, Title 44, U.S.C. § Section 3301 as implemented by Title 36, Code of Federal Regulations, Part 1228; Title 44, U.S.C. § 3310 as implemented by Title 36, Code of Federal Regulations, Part 1229.10.

³ The FBI has subsequently determined file number 100-HQ-446284 was accessioned to NARA on July 21, 2014, and file number 100-NY-157576 was accessioned to NARA on August 2, 2013.

the FOIPA request. Moreover, the FBI informed Plaintiff per standard FBI practice and pursuant to FOIA exemption (b)(7)(E) and Privacy Act exemption (j)(2) [5 U.S.C. §§ 552/552a(b)(7)(E), (j)(2)], its response neither confirms nor denies the existence of Plaintiff's name on any watch lists. Also, the FBI informed Plaintiff he could appeal the FBI's response to the Office of Information Policy ("OIP") within ninety (90) days of the FBI's letter; seek dispute resolution services by contacting the Office of Government Information Services ("OGIS"); and/or contact the FBI's FOIA public liaison. Finally, the FBI informed Plaintiff his FOIPA request was being administratively closed. (Ex. B.)

FBI FOIPA REQUEST NUMBER 1412680-001

(7) By letter dated October 7, 2018, Plaintiff submitted a FOIPA request to the FBI specifically seeking if the FBI has "any Watch Lists from the years 1990-1991 that contain [Plaintiff's] name." (Ex. C.)

(8) By letter dated October 31, 2018, the FBI informed Plaintiff it had assigned his request FOIPA request 1412680-001. Additionally, the FBI informed Plaintiff by standard FBI practice and pursuant to FOIA Exemption (b)(7)(E) and Privacy Act Exemption (j)(2) [5 U.S.C. §§ 552/552a(b)(7)(E), (j)(2)], the FBI can neither confirm nor deny whether a particular person is on any watch list.⁴ Finally, the FBI informed Plaintiff he could appeal the FBI's response to OIP within ninety (90) days of the FBI's letter; seek dispute resolution services by contacting OGIS; and/or contact the FBI's FOIA public liaison. (Ex. D.)

⁴ The FBI did not conduct a search of its records because, in response to Plaintiff's first request, the FBI had already searched for records containing Plaintiff's name and did not find any records in its possession, custody, or control. In addition, unlike Plaintiff's first request, the second request did not refer to any specific meeting or other incident and instead broadly sought to ascertain whether Plaintiff's name appeared on FBI watch lists. The *Glomar* response is the only proper response to such a broad request regarding whether a subject's name appears on watch lists.

(9) By letter dated January 15, 2018,⁵ Plaintiff submitted an appeal to DOJ, OIP challenging the FBI's response to his FOIPA request 1412680-001. (Ex. E.)

(10) By letter sent via email to Plaintiff on August 2, 2019, DOJ OIP informed Plaintiff it affirmed the FBI's actions in response to Plaintiff's FOIA Request Number 1412680-001, therefore, OIP closed Plaintiff's appeal. (Ex. F.) Additionally, OIP informed Plaintiff the FBI properly refused to confirm or deny the existence of any records concerning any individual's placement on any government watch list because their existence is protected from disclosure pursuant to 5 U.S.C. § 552a(j)(2) and 5 U.S.C. § 552(b)(7)(E). Finally, OIP advised Plaintiff if he was dissatisfied with the action on his appeal, Plaintiff could file a lawsuit in federal district court, or seek mediation services from OGIS. (ECF No. 2 at 16-17.)

(11) On January 21, 2020, Plaintiff filed a Complaint in the instant action. (ECF No. 2.)

THE FBI'S CENTRAL RECORDS SYSTEM

(12) The Central Records System ("CRS") is an extensive system of records consisting of applicant, investigative, intelligence, personnel, administrative, and general files compiled and maintained by the FBI in the course of fulfilling its integrated missions and functions as a law enforcement, counterterrorism, and intelligence agency to include performance of administrative and personnel functions. The CRS spans the entire FBI organization and encompasses the records of FBI Headquarters ("FBIHQ"), FBI Field Offices, and FBI Legal Attaché Offices ("Legats") worldwide.

(13) The CRS consists of a numerical sequence of files, called FBI "classifications," which are organized according to designated subject categories. The broad array of CRS file

⁵ Plaintiff's letter may have been inadvertently dated January 15, 2018, instead of January 15, 2019.

classification categories includes types of criminal conduct and investigations conducted by the FBI, as well as categorical subjects pertaining to counterterrorism, intelligence, counterintelligence, personnel, and administrative matters. For identification and retrieval purposes across the FBI, when a case file is opened, it is assigned a Universal Case File Number (“UCFN”) consisting of three sequential components: (a) the CRS file classification number, (b) the abbreviation of the FBI Office of Origin (“OO”) initiating the file, and (c) the assigned individual case file number for that particular subject matter.⁶ Within each case file, pertinent documents of interest are “serialized,” or assigned a document number in the order which the document is added to the file, typically in chronological order.

THE CRS GENERAL INDICES AND INDEXING

(14) The general indices to the CRS are the index or “key” to locating records within the enormous amount of information contained in the CRS. The CRS is indexed in a manner which meets the FBI’s investigative needs and priorities and allows FBI personnel to reasonably and adequately locate pertinent files in the performance of their law enforcement duties. The general indices are arranged in alphabetical order and comprise an index on a variety of subject matters to include individuals, organizations, events, or other subjects of investigative interest that are indexed for future retrieval. The entries in the general indices fall into two category types:

- A. Main entry. A main index entry is created for each individual or non-individual that is the subject or focus of an investigation. The main subject(s) are identified in the case title of most documents in a file.

⁶ For example, in a fictitious file number of “11Z-HQ-56789,” the “11Z” component indicates the file classification, “HQ” indicates that FBI Headquarters is the FBI OO of the file, and “56789” is the assigned case specific file number.

- B. Reference entry. A reference index entry is created for individuals or non-individuals associated with the case but are not the main subject(s) or focus of an investigation. Reference subjects are typically not identified in the case title of a file.

(15) FBI employees may index information in the CRS by individual (persons), by organization (organizational entities, places, and things), and by event (*e.g.*, a terrorist attack or bank robbery). Indexing information in the CRS is done at the discretion of FBI investigators when information is deemed of sufficient significance to warrant indexing for future retrieval. Accordingly, the FBI does not index every individual name or other subject matter in the general indices.

AUTOMATED CASE SUPPORT

(16) Automated Case Support (“ACS”) was an electronic, integrated case management system that became effective for FBIHQ and all FBI Field Offices and Legats on October 1, 1995. As part of the ACS implementation process, over 105 million CRS records were converted from automated systems previously utilized by the FBI into a single, consolidated case management system accessible by all FBI offices. ACS had an operational purpose and design to enable the FBI to locate, retrieve, and maintain information in its files in the performance of its myriad missions and functions.⁷

(17) The Universal Index (“UNI”) was the automated index of the CRS and provided all offices of the FBI a centralized, electronic means of indexing pertinent investigative information to FBI files for future retrieval via index searching. Individual names were recorded with applicable identifying information such as date of birth, race, sex, locality, Social Security

⁷ ACS was and the next generation Sentinel system is relied upon by the FBI daily to fulfill essential functions such as conducting criminal, counterterrorism, and national security investigations; background investigations; citizenship and employment queries, and security screening, to include Presidential protection.

Number, address, and/or date of an event. Moreover, ACS implementation built upon and incorporated prior automated FBI indices; therefore, a search employing the UNI application of ACS encompassed data that was already indexed into the prior automated systems superseded by ACS. As such, a UNI index search in ACS was capable of locating FBI records created before its 1995 FBI-wide implementation in both paper and electronic format.⁸

ACS AND SENTINEL

(18) Sentinel is the FBI's next generation case management system that became effective FBI-wide on July 1, 2012. Sentinel provides a web-based interface to FBI users, and it includes the same automated applications that were utilized in ACS. After July 1, 2012, all FBI generated records are created electronically in case files via Sentinel; however, Sentinel did not replace ACS and its relevance as an important FBI search mechanism. Just as pertinent information was indexed into UNI for records generated in ACS before July 1, 2012, when a record is generated in Sentinel, information is indexed for future retrieval.

(19) On August 1, 2018, the ACS case management system was decommissioned and ACS data was migrated into Sentinel including the ACS indices data and digitized investigative records formerly available in ACS. Moreover, Sentinel retains the index search methodology and function whereby the CRS is queried via Sentinel for pertinent indexed main or reference entries in case files. All CRS index data from the UNI application previously searched via ACS is now searched through the "ACS Search" function within Sentinel.

⁸ Older CRS records that were not indexed into UNI as a result of the 1995 ACS consolidation remain searchable by manual review of index cards, known as the "manual indices."

(20) Upon receipt of FOIPA requests where the subject matter predates the implementation of Sentinel, RIDS predominately begins its FOIPA searching efforts by conducting index searches via the “ACS Search” function in Sentinel. RIDS then builds on its ACS index search by conducting an index search of Sentinel records to ensure it captures all relevant data indexed after the implementation of Sentinel. The CRS automated indices, available within Sentinel and the ACS search function in Sentinel, in most cases represent the most reasonable means for the FBI to locate records potentially responsive to FOIPA requests. This is because these automated indices offer access to a comprehensive, agency-wide set of indexed data on a wide variety of investigative and administrative subjects. Currently, these automated indices consist of millions of searchable records and are updated daily with material newly indexed in Sentinel.

(21) Additionally, the location of records indexed to the subject of a FOIPA request does not automatically mean the indexed records are responsive to the subject. Index searches are the means by which potentially responsive records are located, but ultimately, a FOIPA analyst must consider potentially responsive indexed records against the specific parameters of individual requests. Responsiveness determinations are made once indexed records are gathered, analyzed, and sorted by FOIPA analysts who then make informed scoping decisions to determine the total pool of records responsive to an individual request.

MANUAL INDICES

(22) The indices to the CRS originally consisted of 3”x 5” paper index cards, filed alphabetically based on their subject matter, whether that was an individual, event, organization, or other topic of investigative/administrative interest to the FBI. Along with the subject of interest, these cards also contained the file numbers, serial numbers, and/or pages numbers

within files where the subjects' information was located. The FBI retrieved records by manually searching through these paper index cards, then obtaining the relevant file numbers/serials referenced in the index cards. FBIHQ, each of the FBI's Field Offices, and each of the FBI's Legal Attachés ("Legats") all possessed their own sets of manual index cards.

(23) Much of the FBI's manual indices for FBIHQ and FBI field offices were automated into electronic indices which later merged into ACS; but due to resource constraints and operational needs, not all of the manual indices were originally automated into these electronic indices. This automation for the FBIHQ indices can reasonably be expected to have captured all indexed data on individuals born on or after January 1, 1958, and all organizations/events created/occurring on or after January 1, 1973. The automation for the FBI's field offices can reasonably be expected to capture all indexed data on individuals born on or after June 30, 1973, and all organizations/events created/occurring on or after June 30, 1988. The automation for FBI Legats began with the advent of ACS on October 16, 1995; thus, the FBI determined the automation of Legat indices could reasonably be expected to capture all indexed data on individuals born on or after October 16, 1980, and all organizations/events created/occurring on or after October 16, 1995. If requested records were likely indexed before the timeframes enumerated above, and it is not reasonable for the FBI to assume searches of ACS/Sentinel will locate all indexed data, the FBI conducts searches within the appropriate manual indices.

(24) Starting in April 2008, the FBI began automating its remaining manual indices for FBIHQ, all FBI Field Offices, and all FBI Legats. Automation was accomplished by scanning all of the paper index cards and converting them to digital images. The FBI then used Optical Character Recognition ("OCR") software to make the information on the digital images

electronically searchable. As of December 2010, all of the Manual Indices of FBIHQ, all FBI Field Offices, and all FBI Legats can be searched electronically by FBI personnel.

(25) Considering the Plaintiff's request implicates FBIHQ and field office records on an individual born prior to January 1, 1958, the FBI supplemented its search of the ACS and Sentinel indices with a search of the FBIHQ and New York Field Office ("NYFO") indices.

ADEQUACY OF SEARCHES

(26) Main and Reference Files. RIDS policy is to search for and identify only "main" files responsive to most FOIPA requests at the administrative stage. Subsequent to Plaintiff filing the instant action, RIDS determined an additional search of the CRS to locate any cross-reference files was unnecessary as Plaintiff is challenging only whether his name is or is not on a watch list.

(27) Index Searching. To locate CRS information, RIDS employs an index search methodology. Index searches of the CRS are reasonably expected to locate responsive material within the vast CRS since the FBI indexes pertinent information into the CRS to facilitate retrieval to serve its primary law enforcement and intelligence gathering functions. Given the broad range of indexed material in terms of both time frame and subject matter that it can locate in FBI files, the FBI automated indices available through Sentinel is the mechanism RIDS employs to conduct CRS index searches.

(28) CRS Search and Results. In response to Plaintiff's request, RIDS conducted a CRS index search for potentially responsive records employing the Sentinel and ACS indices available through Sentinel, as well as the manual indices of FBIHQ and NYFO. The FBI searched the following search term: "Henry Plasky." As a result of these search efforts, the FBI located two (2) main files determined to be potentially responsive to Plaintiff's request, which

had previously been sent to NARA. The FBI did not identify any responsive documents in its possession, custody, or control subject to the FOIA.

(29) Scope of Searches. RIDS conducted searches reasonably calculated to locate records responsive to Plaintiff's request. First, given its comprehensive nature and scope, the CRS is the principal records system searched by RIDS, to locate information responsive to most FOIPA requests, because the CRS is where the FBI indexes information about individuals, organizations, events, and other subjects of investigative interest for future retrieval. *See supra* ¶ 14. Second, given that Plaintiff's request seeks information about Henry Platsky, such information would reasonably be expected to be located in the CRS via the index search methodology.

**JUSTIFICATION FOR NON-DISCLOSURE UNDER THE PRIVACY ACT
PRIVACY ACT EXEMPTION (j)(2)**

(30) When an individual requests records about himself/herself from the FBI, we first consider the request under the Privacy Act, which generally provides individuals a right of access to records about them maintained in government files, unless a Privacy Act exemption applies. *See* 5 U.S.C. § 552a. One such exemption is Exemption (j)(2), which exempts from mandatory disclosure systems of records "maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals" 5 U.S.C. § 552a(j)(2). The FBI has exempted law enforcement investigative records maintained in the CRS from the Privacy Act's disclosure requirements pursuant to (j)(2). *See* 63 Fed. Reg. 8671, 8684 (1998).

(31) In response to Plaintiff's request, the FBI determined that if watch list records responsive to Plaintiff existed, they would relate to investigative matters that are part of the

FBI's primary law enforcement mission. Specifically, they would be compiled in furtherance of FBI efforts to track, predict, and thwart terrorist activities. Accordingly, these documents, should they exist, would be exempt from disclosure pursuant to 5 U.S.C. § 552a(j)(2), in conjunction with 28 C.F.R. § 16.96. Although access to any records responsive to Plaintiff's request is denied under the Privacy Act, the FBI also considered whether it could confirm or deny the existence of these records under the FOIA.

JUSTIFICATION OF WATCH LIST *GLOMAR* RESPONSE⁹

(32) The FBI relies on a *Glomar* response in instances in which merely acknowledging the existence or nonexistence of responsive records would result in a harm protected against by one or more FOIA exemptions. To be credible and effective, the FBI must use a *Glomar* response in all similar cases, regardless of whether responsive records actually exist. If the FBI were to invoke a *Glomar* response only when it actually possessed responsive records, the *Glomar* response would be interpreted as an admission that responsive records exist. The FBI determined that merely acknowledging the existence or non-existence of records responsive to parts of Plaintiff's request, other than the records acknowledged, would trigger harms protected by FOIA Exemption 7(E), for reasons explained below.

(33) By supporting the ability of front-line screening agencies to positively identify known or suspected terrorists trying to obtain visas, enter the country, board aircraft, or engage in other activity, the consolidated Terrorist Watch List is one of the most effective

⁹ The term "Glomar response" stems from a case in which a FOIA requester sought information concerning a ship named the "Hughes Glomar Explorer," and the Central Intelligence Agency refused to confirm or deny its relationship with the Glomar vessel because to do so would compromise the national security or divulge intelligence sources and methods. *Phillipi v. CIA*, 655 F.2d 1325 (D.C. Cir. 1981). *Glomar* responses are proper "if the fact of the existence or nonexistence of agency records falls within a FOIA exemption." *Wolf v. CIA*, 473 F.3d 370, 374 (D.C. Cir. 2007).

counterterrorism and law enforcement tools available to the U.S. Government. The Terrorist Watch List is composed of many sub-lists pertaining to various categories of criminal matters under investigation, such as the so-called “No-Fly List.”

(34) It is the FBI’s practice in responding to first party FOIA/Privacy Act requests (*i.e.*, requests by individuals for their own records) to include a standard *Glomar* response that neither confirms nor denies the existence of any watch list information. This *Glomar* response is based on FOIA Exemption 7(E), which protects “records or information compiled for law enforcement purposes [when disclosure] would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.” 5 U.S.C. § 552(b)(7)(E).

EXEMPTION (B)(7) THRESHOLD

(35) Exemption (b)(7) of the FOIA protects from mandatory disclosure records or information compiled for law enforcement purposes, but only to the extent that disclosure could reasonably be expected to cause one of the harms enumerated in the subpart of the exemption. See 5 U.S.C. § 552 (b)(7). In this case, the harm that could reasonably be expected to result from disclosure concerning the release of techniques and procedures which could reasonably be expected to risk circumvention of the law.

(36) Before an agency can invoke any of the harms enumerated in Exemption (b)(7), it must first demonstrate that the records or information at issue were compiled for law enforcement purposes. Law enforcement agencies such as the FBI must demonstrate that the records at issue are related to the enforcement of federal laws and that the enforcement activity is within the law enforcement duty of that agency. Pursuant to 28 USC §§ 533, 534, and Executive

Order 12333 as implemented by the Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM) and 28 CFR § 0.85, the FBI is the primary investigative agency of the federal government with authority and responsibility to investigate all violations of federal law not exclusively assigned to another agency, to conduct investigations and activities to protect the United States and its people from terrorism and threats to national security, and further the foreign intelligence objectives of the United States. The FBI's records concerning terrorist watch lists were compiled and created in furtherance of the FBI's law enforcement, national security, and intelligence missions. To accomplish these missions, inherent tasks and operational functions are required, to include the identification of, development, and implementation of law enforcement, counterterrorism, and intelligence gathering methods, techniques, and procedures. Specifically, information contained on the terrorist watch list is used as a method and technique that has enabled the FBI to perform its core law enforcement and national security missions. Accordingly, the records related to the FBI's use of the terrorist watch list readily meets the threshold requirement of Exemption (b)(7). The remaining inquiry is whether disclosure of certain information pertaining to FBI techniques and procedures could reasonably be expected to risk circumvention of the law.

(B)(7)(E) INVESTIGATIVE TECHNIQUES AND PROCEDURES

(37) 5 U.S.C. § 552(b)(7)(E) provides for the withholding of:

law enforcement records [which]...would disclose techniques and procedures for law enforcement investigations or prosecutions or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

(38) In order for this exemption to apply, the specifics of the use of the technique or procedure at issue must not be well-known to the public. However, even commonly known

techniques or procedures may be protected from disclosure if the disclosure of details about the commonly known procedure could reduce or nullify its effectiveness.

Acknowledgment Alone Triggers Harm

(39) The FBI asserted FOIA Exemption (b)(7)(E), to neither confirm nor deny that Plaintiff's name is on any watch list. Given the sensitive information contained in the watch list, the mere acknowledgement of the existence or non-existence of responsive records would trigger harm. Revealing this fact alone could enable the targets of the watch list to avoid detection or to develop countermeasures to circumvent the ability of the FBI to effectively use this important law enforcement technique, therefore, allowing circumvention of the law.

(40) Although the existence of No-Fly lists became public in October 2002, the specific criteria and standards for placing individuals on watch lists have not been made publicly known. In late 2004, the White House Homeland Security Council ("HSC") approved new criteria for inclusion of individuals on No-Fly lists. The Terrorist Screening Center ("TSC")¹⁰

¹⁰ The Terrorist Screening Center ("TSC") was created pursuant to Homeland Security Presidential Directive-6 ("HSPD-6") and began operations on December 1, 2003. The TSC is administered by the FBI with support from the intelligence community, Department of Justice, Department of Homeland Security, Department of State, Department of Treasury, and Department of Defense. Its mission is to coordinate the Government's approach to terrorism screening and to maintain a consolidated database of all known and suspected terrorists for use in screening. Prior to creation of the TSC, information about known and suspected terrorists was dispersed throughout the U.S. government, and no single agency was responsible for consolidating and making the terrorist watch lists available for use in screening. In March 2004, the TSC consolidated the Government's terrorist watch list information into a sensitive but unclassified database known as the TSDB. As required by HSPD-6, the TSDB contains "information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism." Information from the TSDB is used to screen for known and suspected terrorists in a variety of contexts, including during law enforcement encounters, the adjudication of applications for U.S. visas or other immigration and citizenship benefits, at U.S. borders and ports of entry, and for civil aviation security purposes.

prepared a list of terrorist subjects who were assigned to these lists within the Terrorist Screening Center Database (“TSDB”), and the FBI’s Joint Terrorism Task Force (“JTTF”) case agents and other nominating agencies reevaluated their subjects’ status and adjusted status as appropriate to comply with the new criteria. In January 2005, TSC implemented guidance for placing individuals on No-Fly lists. The guidance provides specific criteria for nominating individuals for No-Fly lists and includes examples of appropriate and inappropriate nominations, which are tied directly to aviation security and terrorism.¹¹ The specific criteria cannot be made public without compromising intelligence and security or inviting subversion of these lists by individuals who will seek ways to adjust their behavior to avoid being identified as a threat to aviation. Thus, the success of this anti-terrorism tool depends in part on the confidentiality of the protocols for inclusion on a No-Fly list.

(41) The rationale behind the FBI’s Exemption 7(E) *Glomar* response with regard to government watch list records, is that to confirm Plaintiff or any individual’s watch list status reasonably could be expected to compromise investigative operations as well as endanger investigative or intelligence sources and methods. For example, confirming that any particular individual is listed in the TSDB could heighten an individual’s suspicion, inducing him or her to more closely scrutinize activities and associations, which in turn would compromise highly sensitive methods and sources. Such official confirmation could, in turn, induce an individual to flee, destroy or hide evidence, alter his or her own behavior, or it may cause his or her close associates to alter their behaviors in order to avoid detection by law enforcement. Conversely,

¹¹ DHS Privacy Office Report Assessing the Impact of the Automatic Selectee and No-Fly Lists on Privacy and Civil Liberties (April 27, 2006)

confirmation that an individual is not on a watch list tends to suggest that the individual's actions have not come under scrutiny.

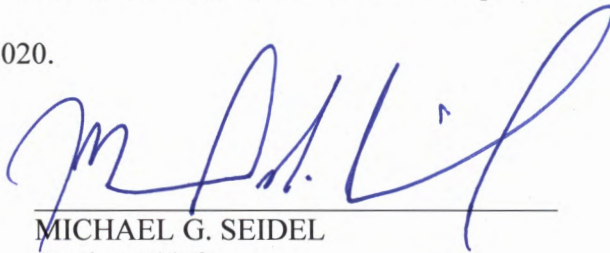
(42) It is not sufficient for the FBI to issue a *Glomar* response to individuals in response to only certain requests (for example, those requests by individuals who are on a watch list), because that differential treatment could itself be telling. Moreover, as pieces of information about who is or is not (or may or may not be) on a watch list becomes known, adversaries can begin to construct a picture of what types of behavior are pertinent to placement on a watch list and the extent to which the government is aware of adversaries and their activities. Such information would then allow them to develop countermeasures to conceal their activities and thwart efforts to interdict crime and protect the national security of the United States. Thus, the government has determined that a consistent, across-the-board *Glomar* response—pursuant to Privacy Act Exemption (j)(2) and FOIA Exemption (b)(7)(E)—to all first-party requests under the FOIPA, neither confirming nor denying any individual's watch list status, is the best way of ensuring that the harms discussed above do not occur.

CONCLUSION

(43) The FBI performed adequate searches reasonably likely to locate records responsive to Plaintiff's request subject to the FOIA. Those searches identified potentially responsive records which had previously been sent to NARA, and the FBI's response in this regard was proper. Finally, the FBI appropriately issued a *Glomar* response pursuant to Privacy Act Exemption (j)(2) and FOIA Exemption (b)(7)(E) that neither confirms nor denies Plaintiff's status on a government watch list.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct, and that Exhibits A through C attached hereto are true and correct copies.

Executed this 22nd day of October, 2020.



MICHAEL G. SEIDEL
Section Chief
Record/Information Dissemination Section
Information Management Division
Federal Bureau of Investigation
Winchester, Virginia